

## CIPHERING COMMUNICATION SYSTEM

Patent Number: JP9200195

Publication date: 1997-07-31

Inventor(s): NAKAMURA MICHIIRO

Applicant(s):: BROTHER IND LTD

Requested Patent:  JP9200195

Application Number: JP19960010104 19960124

Priority Number(s):

IPC Classification: H04L9/18 ; G09C1/00 ; H04L9/34

EC Classification:

Equivalents:

### Abstract

**PROBLEM TO BE SOLVED:** To attain high speed transmission of ciphered data by using a ciphering key so as to apply decode processing to received ciphered data and synthesizing divided data in the order of numbers.

**SOLUTION:** A transmitter side informs ciphering communication to a receiver side, received transmission data are divided for 512-byte each by a data division section 2 and numbers 1-N are provided to the divided data in the division order and the resulting data are stored in a data storage section 3. The ciphered data are sent from a data transmission section 8 in order. The ciphered data are received by a data reception section 10 and decoded by a decoding section 12 by using a common shared ciphering key and stored in a data storage section 13. The stored data are synthesized in the order of division numbers for each page by a data synthesis section 14. The synthesized data are outputted by a data output section 15 and the entire transmission signal data are outputted finally.

Data supplied from the esp@cenet database - I2



が送達される。呼号データの送信が完了すると、終了メッセージを送信して通信を終了する (S10)。

(10019) 図3は本実施形態における呼号送信方式の受信処理手順を示すフローチャートである。

(10020) 送信段階の際に呼号送信が通知されると (S21: Y)、受信側の呼号記憶が呼号送信行部9で片流れ (S22)、呼号データの受信準備が完了する。

(10021) 呼号ビデータは、データ受信部10によつて受信されると共に (S23)、片付けられた呼号頭を用いてデータ呼号ビデータ12によつて削除処理され (S24)、データ受信部13に蓄積される。蓄積されたデータは、図4に示すフォームットであるので、データ合成功部14によつて分割呼号の順序にページ単位に合成される (S25)。合成されたデータはデータ出力部15によって出力される (S26)。最終的に送信データ全体を出力することができる。送信データメッセージを受信する。

(10022) このように、送信データに比べて分割データは小さいので、呼号ビデータは直ち時間で完了して送信されるので送信開始までの時間を見くくることができ、メッセージに亘る文書等の場合には、断次呼号データの呼び出し処理を行うことができ、ページ単位間に合流を行つて出力するので、送信データ全体を一度に呼び出し処理するよりも高速に呼号データの送信・出力をを行うことができる。

[0023] また、前記英施の形態では、データの分割サイズは512バイトであるが、他の分割サイズでも可能であり、履歴の分割データのサイズ調整のためにアスキコードの「0x20」を追加しているが、「0x00」が他のコードでも可能である。また、仮想データの合流はページ単位で行っているが、復元されたデータを結合せずに直次出力することも可能である。

による研究評議の場合は、アカシミリ通感にこの研究評議方式を適用することももちろん可能である。

【0025】また、分別データをそれぞれ異なる瞬時測定を行い、暗号化データとすることも可能である。

【0026】次に、本実例を具体化した他の実施の形態について図2及び図3を参照して説明す

[0027] 先ず、送信側では、コンピュータで作成された送信データがデータ入力部1により入力され(S2:1)、送信者によって明示・暗示が選択されれば(S2:2)、暗号送信手順を行い、暗号送信が選択されなければ(S2:3)、暗号送信手順を行ない、暗号送信が選択されれば(S2:4)、送信の暗号を用意しない通常が行われる。暗号送信の場合には(S2:5)、要件側との通信接続の際に、暗号送信の通知が受件側に通知される。(S2:6)

3) 入力された送信データを4096バイトと仮定し、行列を1バイト単位として、 $N = 64$ 、 $M = 64$ とすると、送信データは図5のように示される。この送信データは、データ分割部2において分割処理され(5行目)、1列目のデータは、  
 $D1 = M1N1, M1N2, M1N3, \dots, M1N$

[0021] 営号データは、データ受信部10によつて受信されると共に(S23)、共有された暫号処理を用いてデータ復号部12によつて復号処理され(S24)、データ布話部13に蓄積される。蓄積されたデータは、図4に示すフォーマットであるので、データ合成功能は、図4以下送信データは、次64列目のデータまで同様に分割される。

[0029] D4=M64N1, M64N2, M64N3, ..., M64N64

ここで、これらの64個に分割されたデータは、分割されたデータは、データ受信部10によつて受信されると共に(S23)、共有された暫号処理を用いてデータ復号部12によつて復号処理され(S24)、データ布話部13に蓄積される。蓄積されたデータは、図4に示すフォーマットであるので、データ合成功能は、図4以下送信データは、次64列目のデータまで同様に分割される。

られた順番に 1 ~ 6 4 の分割番号が付けられ、图 6 のようなフォーマットで分割データに追加されて、データ番号部 3 に蓄積される (S 5)。

(0030) データの暗号化処理に使用される暗号鍵は、 $N = 6$  4 分だけ暗号鍵生成部 5 で作成され (S 6)、暗号鍵共有部 6 で公開鍵暗号方式を用いて受信側に送信され、受信側と暗号鍵の共有を行 (S 7)。この暗号鍵の共有が完了すると、データ暗号化部 4 において分割暗号を含めた分割データを暗号鍵を用いて暗号化し (S 8)、暗号化されたデータを暗号部 7 でデータ送信部 8 から受信側に送信する (S 9)。この時、暗号化部 7 は、  
 (0027) より、送信データに比べて分割データ  
 (0022) は小さいので、暗号化処理は短い時間で完了して送信されるので分割暗号までの時間は短くすることができ、  
 (0021) レジストが等の場合には、暗号化データの以  
 后処理を行うことができ、ヘージ単位間に分成して  
 (0020) 出力するので、送信データ全体を一度に暗号化処理する。  
 (0019)

る。

[0023] また、前記実施の形態では、データの分割サイズは512バイトであるが、他の分割サイズでも可能であり、仮想の分割データのサイズ調整のためにアクセスコードの“0×20”を使用しているが、“0×00”その他とのコードでも可能である。また、仮想データの合はベース位置で行っているが、假想されたデータを合成せずに取出出力することも可能である。

[0024] 一方、前記実施の形態では、データの分割データが暗号化処理される時にはロー1個目の暗号データが送信される。暗号データの送信が完了すると符号メッセージを送信して通信を終了する(S10)。

[0031] 受信側では、通信接続の際に暗号鍵が通知(S21:Y)されると、受信側の暗号鍵が暗号鍵と共に右部9で共有され(S22)、暗号化データの受信準備が完了する。

による暗号通信の場合について述べたが、ファシリミリ通信にこの暗号通信方式を使用することももちろん可能である。

(0025) また、分割データをそれぞれ異なる暗号復用して暗号化処理を行い、暗号化データとすることも可能である。

(0026) 次に、本例を具体化した他の実施の形態について図2及び図3を参照して説明する。

[0027] 先ず、送信側では、コンピュータで作成された送信データがデータ入力部1により入力され(S0031)、送信者によって呼び出し履歴が選択されれば(S0032)、呼び出送信手順を行い、呼び出し履歴が選択されなければ(S0033)、呼び出送信手順を行い、呼び出し履歴が選択されれば(S0034)、通常の呼び出しが行われる。呼び出し履歴の場合には(S0035)、受信側との通信依頼の際に、呼び出し履歴の通知が受信側に通知される(S0036)。受信側は、送信データをN行×N列のデータに分割し、各列毎にデータを合成してひとつつの分割データとし、この分割データをそれぞれ異なる暗号領域用いて暗号化処理を行うことにより、より暗号強度の高い暗号通信を行うことが可能となる。

は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データをハイパット単位でN×M個に分割して、その各列毎に列方向のデータを合流することにより、 $N \times M$  バイトのデータを作成して、各列のデータ毎に $(1 \leq i \leq M)$  の番号を付けて置く一方、そのM列と同様の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データ

データをそれをそれそれ応する前記暗号題用いて暗号化処理した後、その各暗号データを前記M回分繰り返して受信側にて送信し、前記受信側では、受信した前記各暗号データを前記受信側と併存する前記各暗号題用いて復号化処理する。この技術は、たとえば、[特許第4111111号](#)に記載の如くである。

[0 0 0 9] [解説の英施の形態] 以下に、本拠明の暗号通信方式を具体化した実施の形態について図面を参照して説明する。

[0 0 1 0] 図1は本実施の形態における暗号通信方式の構成を示すブロック図である。

[0 0 1 1] データを送信する送信側は、データ入力部1、データ分割部2、データ送信部3、データ暗号化部4、

4、暗号化生成部5、送信側制御部6、暗号化部7、データ送信部8等から構成されている。  
 [0012] 前記データ入力部1は、入力装置（例えは、キーボード等）からデータを入力する装置である。前記データ入力部1は、前記データ出力部2に分入されたデータを51.2バイト毎のデータの形態で出力するものであり、分割データの最後のものには、ちょうど51.2バイトになるよう付加データとして、アスキーキャリコードの“空白”文字を終わらす“0x20”（16

を追加して12バイトにする機能を有するようにしている。前記データ破壊部3は、データ分割部2で分割された各データに付与された順番に分割番号を付け分離するものである。前記データ破壊部4は、分割番号が付けられた分割データを暗号処理して暗号化処理するものであり、分割データは分割番号と一緒に暗号化されるものである。前記データ生成部5は、暗号化処理を行うための暗号鍵を生成するためのものであって、

（参考文献）  
〔1〕「送信側の制御処理全体を実行するものであり、データ符号化処理の制御側の制御部、暗号化生成部、データ符号化処理の制御、受信側との符号通信は有効である」としている。  
〔2〕「前記送信側制御部6は、送信側の制御処理全体を実行するものであり、データ符号化処理の制御部、暗号化生成部の制御、受信側との符号通信は有効である。前記受信側制御部7は、前記送信側制御部6で生成された暗号情報を受信側で検出するための処理を行つるものであつて、公開鍵暗号方式を用いて検出する」としている。

用いて暗号処の共有を行うものである。前記データ送信部8は、データを受信側に送信する処理を行うものである。

[0014]一方、本実施形態の受信側は、暗号処理部9、データ受信部10、受信制御部11、データ符号化部12、データ送部13、データ合成功部14、データ出力部15等から構成される。

前記データを受信する処理を行なうものである。前記受信部11は、骨伝導の制御処理全般を実行するものである。

の送信処理手順を示すフローチャートである。  
（10017）先ず、送信側では、コンピュータで作成された送信データがデータ入力部1により入力され（S1）、送信者によって送信データを示す。（以下同様）、送信者が選択されれば（S2：Y）、符号送信手順を実行し、符号送信が選択されなければ（S2：N）、通常の順序で操作が行われる。符号送信の場合に、符号送信の通知が受信側に通知される（S3）。入力された送信

データは、512バイト西にデータ分割部2で分割される（S4）。この時、分割されたデータの最後の分割データがちょうど512バイトになるように最終分割データは、N個に分割される。ここで、N個に分割されたデータは、N個の分割部3に送信される（S5）。

【0018】データの符号処理に使用される符号は、データ分割部5で作成され（S6）、呼び出し共有部7で

記入部では、受信した前記各暗号化データを前記受信側と共に行する前記各暗号化用いて仮想処理し、その処理された分割データを前記N行×M列に合成するようにして、分割した分割データをそれそれ異なる暗号処理暗号化することにより、データの機密性が一番高い暗号処理を行うことができる。

【図面の簡単な説明】

【図1】本発明の実施の形態における暗号通信方式的情報を示すブロック図である。

【図2】暗号通信方式の送信手順を示すフローチャートである。

【図3】暗号通信方式の受信手順を示すフローチャートである。

【図4】暗号通信方式の分割データのフォーマットを示す図である。

【図5】本発明の他の実施の形態における暗号通信方式のN行×M列の分解データのフォーマットを示す図である。

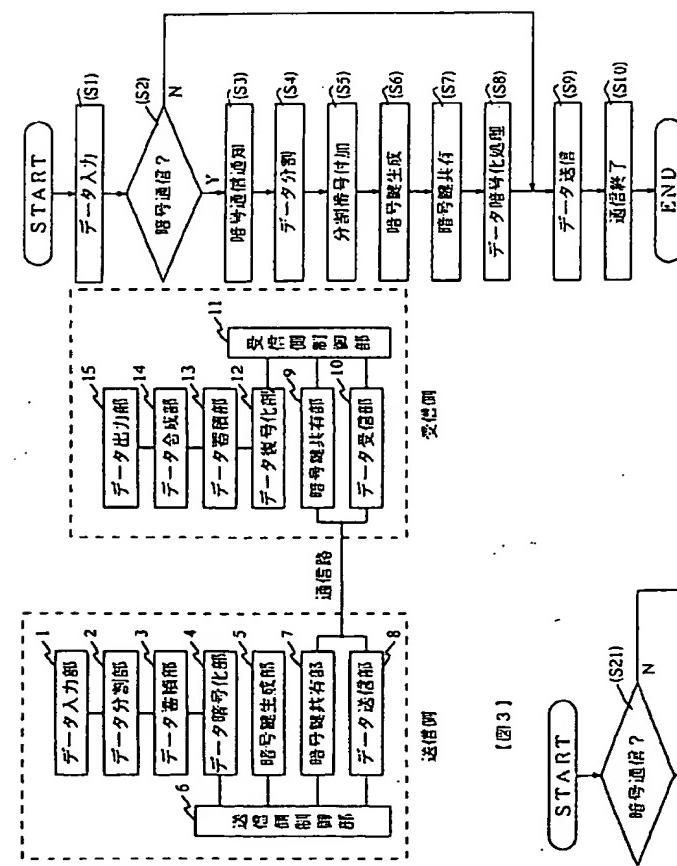
【図6】他の実施の形態における暗号通信方式の分割データのフォーマットを示す図である。

【符号の説明】

- 1 データ入力部
- 2 データ分割部

応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記N回分繰り返して受信側に送信し、前記

1



四

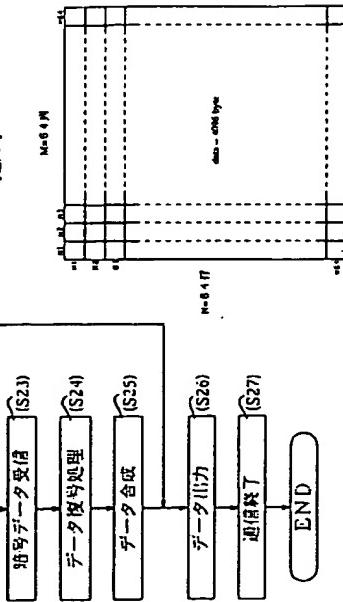
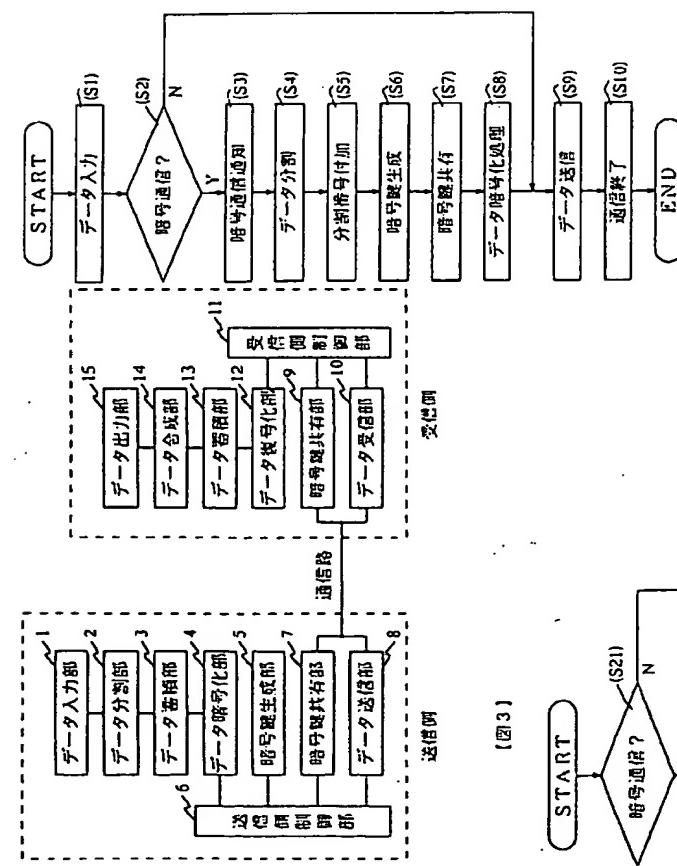
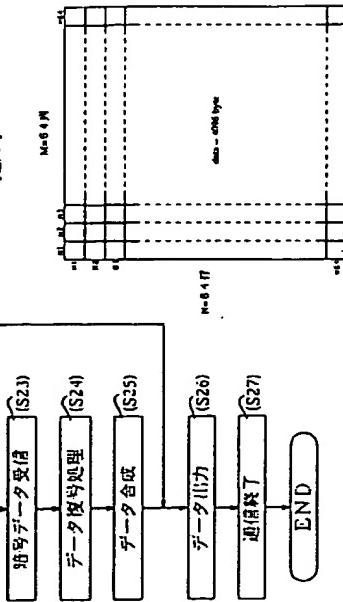


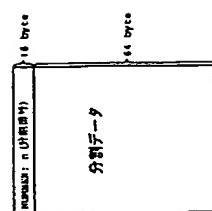
图21



四



一〇四



11